

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

MICHAEL WEINGAND,

No. C-11-3109 EMC

Plaintiff,

v.

**ORDER GRANTING DEFENDANT'S
MOTION FOR LEAVE TO FILE
AMENDED ANSWER**

HARLAND FINANCIAL SOLUTIONS,
INC., *et al.*,

(Docket No. 29)

Defendants.

Plaintiff Michael Weingand filed suit against Harland on June 23, 2011, alleging claims of, *inter alia*, wrongful termination and employment retaliation. On April 17, 2012, Defendant Harland Financial Solutions (“Harland”) filed a motion for leave to file an Amended Answer, adding counterclaims for violations of the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030; California Penal Code § 502; conversion; breach of contract; unjust enrichment; negligent interference with prospective economic advantage; and California Business and Professions Code § 17200. Docket No. 30, Ex. 18.

After reviewing the parties’ submissions, and for the reasons set forth below, the Court **GRANTS** the motion.

I. FACTUAL AND PROCEDURAL BACKGROUND

Harland’s proposed counterclaims are based on Defendant’s allegations that, after his employment with Harland as a Senior Field Engineer was terminated, Plaintiff “accessed, without authorization, over 2,700 business files belonging to Harland, its clients, and/or third-party software vendors some or all of which contained NPI [non-public information], copyrighted information,

and/or confidential and propriety information.” Am. Ans. ¶ 14. Defendant also alleges that Plaintiff accessed and copied Harland’s licensed OnBase software, which it contends he now uses in his own business after he was terminated from Harland. *Id.* ¶¶ 18-19. Defendant alleges that Plaintiff thereby violated his obligation to “maintain the secrecy of Harland’s confidential and proprietary information not only while employed by Harland but also after his employment ended.” Am. Ans. ¶ 9.

The parties have engaged in discovery since June 2011. According to Defendant, it has been in the process of developing the basis for its counterclaims since October 2011. Most recently, Defendant informed the Court at the March 16, 2012 case management conference that it intended to assert counterclaims. The Court’s minute order from that conference directed Defendant to obtain Plaintiff’s stipulation or file a motion for leave to amend no later than April 17, 2012, the date on which Defendant filed the instant motion. *See* Docket No. 26. Defendant sought a stipulation from Plaintiff, which Plaintiff refused to provide. *See* Svanfeldt Decl., Docket No. 30, Ex. 17.

II. DISCUSSION

A. Legal Standard

Generally, leave to amend pleadings “shall be freely given when justice so requires.” Fed. R. Civ. P. 15(a). To assess a motion for leave to amend, the court considers “the presence of any of four factors: bad faith, undue delay, prejudice to the opposing party, and/or futility.” *See Owens v. Kaiser Foundation Health Plan, Inc.*, 244 F.3d 708, 712 (9th Cir.2001); *see also Foman v. Davis*, 371 U.S. 178, 182 (1962) (in the absence of any “apparent or declared reason-such as undue delay, bad faith or dilatory motive, ... undue prejudice to the opposing party, ... futility of amendment, etc.,” leave should be freely given). Plaintiff opposes Defendant’s motion for leave to amend on the basis of futility, undue delay, and prejudice.

B. Futility

Plaintiff argues that amendment would be futile because Defendant’s counterclaims would be subject to a Rule 12(b)(6) motion to dismiss. “A proposed amendment is futile only if ‘no set of facts can be proved under the amendment that would constitute a valid claim or defense.’” *Echostar Satellite LLC v. Freetech, Inc.*, C 07-06124 JW, 2009 WL 8398696, at *1 (N.D. Cal. July 7, 2009)

(quoting *Miller v. Rykoff-Sexton, Inc.*, 845 F.2d 209, 214 (9th Cir. 1988)); *see generally* 6 Fed. Prac. & Proc. Civ. § 1487 (3d ed.) (“[I]f a complaint as amended could not withstand a motion to dismiss or summary judgment, then the amendment should be denied as futile.”).

1. CFAA

First, with respect to Defendant’s CFAA claim, Plaintiff argues it fails to state a claim because the CFAA only provides for a private right of action if the violation has caused

(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value;

(II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(III) physical injury to any person;

(IV) a threat to public health or safety; [or]

(V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security.

18 U.S.C. § 1030(g). Plaintiff argues the proposed amended counterclaim offers no allegations to support any of these criteria. Opp. at 4. In addition, Plaintiff contends the counterclaim offers no allegations that Defendant’s computer is a “protected computer” under the statute. § 1030(e)(2).

However, the counterclaim plainly contains both allegations regarding damages and allegations that the computer in question was a “protected computer.” *See* Am. Ans. ¶ 24 (“Harland’s computer is deemed a “protected computer” as defined by the CFAA in that it is used by Harland in a manner that affects interstate or foreign commerce or communication.”); *Id.* ¶ 26 (“As a direct and proximate result of Weingand’s conduct, Harland suffered and continues to suffer damages in an amount exceeding \$5,000 within a one year period including, but not limited to, the costs of conducting an investigation into Weingand’s unauthorized access and conduct, the costs of conducting a damage assessment, the costs and reputational harm associated with notifying customers of Weingand’s conduct and unauthorized access, and the cost of taking corrective action

1 based on Weingand's conduct, such amounts to be determined according to proof at trial.")).

2 Plaintiff's first argument with respect to the CFAA fails.

3 Plaintiff's remaining argument, that the counterclaim contains no allegations as to how
4 Plaintiff's access was unauthorized, is similarly unpersuasive. Defendant states specifically that
5 Plaintiff received permission to access Harland's computer system based on his representations that
6 he sought to get his "personal files" after his termination, but that he had no authority with respect to
7 the additional files he accessed. Thus, the counterclaim creates at least a reasonable inference that
8 his authorization extended only to accessing and copying said "personal files" and that he exceeded
9 that authorization. *See United States v. Nosal*, 676 F.3d 854, 857 (9th Cir. 2012) ("[A]ssume an
10 employee is permitted to access only product information on the company's computer but accesses
11 customer data: He would 'exceed [] authorized access' [as defined in § 1030(e)(6)] *if he looks at the*
12 *customer lists.*") (emphasis added); *Cf. Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 967-68
13 (D. Ariz. 2008) (holding that "a violation for 'exceeding authorized access' occurs where initial
14 access is permitted but the access of certain information is not permitted," and dismissing CFAA
15 claim because "Shamrock conceded that Gast was permitted to view *the specific files* he allegedly
16 emailed to himself") (emphasis added) (citations omitted); *Diamond Power Int'l, Inc. v. Davidson*,
17 540 F. Supp. 2d 1322, 1342-43 (N.D. Ga. 2007) (construing "exceed[ing] authorized access" to
18 include "an employee who accesses a computer with initial authorization but later acquires (with an
19 improper purpose) files to which he is not entitled," and dismissing CFAA claim because "[t]here is
20 [] no dispute that his level of authorized access included express permission (and password access)
21 to obtain *the specific information* he later disclosed") (emphasis added).

22 Although Plaintiff's counsel contended at oral argument that Plaintiff's level of *verbal* (or
23 non-technical) authorization was irrelevant because the only "authorization" to which the statute
24 speaks is "code" authorization (*i.e.*, whether someone is literally blocked from certain files by some
25 security measure such as a password), Plaintiff offers no authority to support such a narrow
26 interpretation. It is true that *Nosal* uses the phrase "physical access" to describe the expansive
27 interpretation of the CFAA the government proposed (and the court rejected). *Nosal*, 676 F.3d at
28 857 (rejecting the government's proposition that "the language could refer to someone who has

1 unrestricted physical access to a computer, but is limited in the use to which he can put the
2 information”). However, the previous sentence of the opinion makes clear that the court was
3 concerned only with the distinction between access and use, not with any distinction between types
4 of authorization pertaining to access. *Id.* (noting that “an employee [would exceed authorized access
5 if he] is *permitted* to access only product information on the company’s computer but accesses
6 customer data”) (emphasis added). Indeed, the fact that *Nosal* uses the word “authorization”
7 interchangeably with “permission,” suggests that one need not engage in such rigorous technological
8 measures to block someone from accessing files in order to limit their “authorization.” *See id.* at
9 864 (“Because Nosal’s accomplices had *permission* to access the company database and obtain the
10 information contained within, the government’s charges fail to meet the element of ‘without
11 authorization, or exceeds authorized access’ under [the CFAA].”) (emphasis added).

12 Previous Ninth Circuit authority (un-altered by *Nosal*) indicates that if a former employee
13 accesses information without permission, even if his prior log-in information is still operative as a
14 technical matter, such access would violate the CFAA. *LVR Holdings LLC v. Brekka*, 581 F.3d
15 1127, 1136 (9th Cir. 2009) (“There is no dispute that if Brekka accessed LVR’s information on the
16 LOAD website after he left the company in September 2003, Brekka would have accessed a
17 protected computer ‘without authorization’ for purposes of the CFAA.”).

18 Thus, although *Nosal* clearly precluded applying the CFAA to violating restrictions on *use*, it
19 did not preclude applying the CFAA to rules regarding *access*. Nor did it speak to the situation
20 presented here, where Plaintiff was no longer employed by Defendant and allegedly no longer had
21 generalized authorization or permission to access files, including the files in question. Moreover,
22 the exact nature and scope of Plaintiff’s authorization as a factual matter (verbal, physical, or
23 otherwise), is not properly before the Court based on the pleadings alone, and thus a precise
24 delineation of whether the events in question may or may not be covered under the statute is
25 premature on this Rule 15 motion.

26 Accordingly, amendment to add the CFAA claim is not futile. *See Jun Han v. Futurewei*
27 *Technologies, Inc.*, 11-CV-831-JM JMA, 2011 WL 5118748 (S.D. Cal. Oct. 28, 2011) (so finding
28

1 under similar facts regarding unauthorized access to a work computer as a counterclaim against a
2 former employee).

3 2. Penal Code § 502

4 Plaintiff next argues that Defendant's California Penal Code § 502 claim is futile because §
5 502 applies only to activities related to "hacking," while Plaintiff was explicitly granted access from
6 Harland's employee Julie Vernali. Opp. at 4. Plaintiff cites to *People v. Gentry* for support, which
7 states that "[o]ne of the legislative purposes of Penal Code section 502 was "to deter and punish ...
8 browsers and hackers-outsiders who break into a computer system to obtain or alter the information
9 contained there. ..." *People v. Gentry*, 234 Cal. App. 3d 131, 141 n.8 (1991) (citation omitted).
10 However, *Gentry* does not necessarily indicate that the statute targets only "hackers" as Plaintiff
11 would define them (*i.e.*, people who obtain access from offsite or through breaking through some
12 kind of security system). *See also Mahru v. Superior Court*, 191 Cal. App. 3d 545, 449 (1987)
13 (describing legislative declaration regarding the need to deter "unauthorized intrusions into
14 computer systems" as not conclusive of a "legislative intent to deter and punish only browsers and
15 hackers"; concluding instead that the court "cannot be confident that this brief declaration of
16 purpose was intended to summarize every act covered by the statute").

17 Nor do the additional cases Plaintiff cites foreclose Defendant's cause of action under the
18 statute. For example, *People v. Lawton*, cited by Plaintiff, held that "permissible use of hardware to
19 access impermissible levels of software is a violation of that section." 48 Cal. App. 4th Supp. 11, 14
20 (1996). Although the specific facts in *Lawton* indicated that the defendant had used his permitted
21 access (to a public library computer terminal) "to bypass security and penetrate levels of software
22 not open to the public," *id.* at 12, the Court of Appeal did not purport to limit § 502's application to
23 unauthorized access that involved bypassing security. Rather, the court's holding focused on the
24 definition of "computer system" and "computer network" and concluded that *authorized* access to a
25 portion of a computer system (*i.e.*, its hardware) did not preclude a finding that one had obtained
26 *unauthorized* access to another portion of that system (*i.e.*, certain software). *Id.* at 15. Similarly,
27 although *Chrisman v. City of Los Angeles*, 155 Cal. App. 4th 29 (2007) supports Plaintiff's
28 construction in that it held § 502 did not apply to an officer's misuse of his work computer "to get

1 information to which he was entitled when performing his job, but retrieved it for non-work-related
2 reasons,” it is distinguishable because *Chrisman* concerned the misuse of computers to which the
3 employee had authorized access while he was still employed, whereas Defendant contends that
4 Plaintiff accessed without permission the software and data after his employment was terminated.
5 155 Cal. App. 4th at 35.

6 As stated above, the Court in *United States v. Nosal* held “that the phrase ‘exceeds
7 authorized access’ in the [federal] CFAA does not extend to violations of use restrictions,” only to
8 access violations, but would include accessing without authorization particular files and databases,
9 not just full computer systems. It would appear that § 502, if anything, covers at least as broad a
10 range of unauthorized *access* to information as the CFAA. *Compare* Cal. Penal Code § 502(c)(2)
11 (defining a public offense as occurring when one “[k]nowingly accesses *and without permission*
12 *takes*, copies, or makes use of any data from a computer . . .”) (emphasis added), *with* 18 U.S.C. §
13 1030(a)(2)(C) (defining offense as occurring when one “intentionally *accesses a computer without*
14 *authorization* or exceeds authorized access, and thereby obtains . . . information from any protected
15 computer”) (emphasis added). Thus, *Nosal* supports the application of § 502 here.¹

16 Other case law supports Defendant’s use of the statute for this type of claim. *See Facebook,*
17 *Inc. v. ConnectU LLC*, 489 F. Supp. 2d 1087, 1091 (N.D. Cal. 2007) (Seeborg, J.) (“As the FAC
18 alleges facts showing that ConnectU knowingly accessed Facebook’s website to collect, copy, and
19 use data found thereon in a manner not authorized or permitted by Facebook, the motion to dismiss
20 will be denied as to this [§ 502] claim.”); *Han*, 2011 WL 5118748 at *1 (finding Defendant stated a
21 claim under § 502 by alleging former employee “illegally copied and deleted various files from her
22 company-issued laptop during the summer of 2010”). Notably, in *ConnectU*, the defendant had
23 accessed “information on the Facebook website that ordinarily would be accessible only to
24 registered users by using log-in information voluntarily supplied by registered users.” 489 F. Supp.
25 2d at 1091. Thus, ConnectU did not “hack” into the website because it used valid log-in information

26
27 ¹ “Although cases interpreting the scope of liability under the CFAA do not govern the
28 Court’s analysis of the scope of liability under Section 502, CFAA cases can be instructive.”
Facebook, Inc. v. Power Ventures, Inc., C 08-05780 JW, 2010 WL 3291750, at *9 (N.D. Cal. July
20, 2010).

1 supplied by others. The court was unpersuaded by this distinction because ConnectU acted without
2 authorization from Facebook to retrieve the information it retrieved. *Id.* (“[N]otwithstanding the
3 reference in the title to “unauthorized access,” Penal Code section 502 prohibits *knowing* access,
4 followed by *unauthorized* (i.e., “without permission”) taking, copying, or use of data.”) (emphasis in
5 original); *see also DocMagic, Inc. v. Ellie Mae, Inc.*, 745 F. Supp. 2d 1119, 1151 (N.D. Cal. 2010)
6 (following *ConnectU* under similar facts).

7 The Court notes that at least one Judge in this District has declined to follow *ConnectU* and
8 instead set a threshold under § 502 that defines unauthorized access as “that [which] circumvents
9 technical or code-based barriers that a computer network or website administrator erects to restrict
10 the user’s privileges within the system, or to bar the user from the system altogether.” *Facebook,*
11 *Inc. v. Power Ventures, Inc.*, C 08-05780 JW, 2010 WL 3291750, at *11 (N.D. Cal. July 20, 2010);
12 *see also In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 715-16 (N.D. Cal. 2011) (applying
13 same rule from *Power Ventures* in another case before the same judge). Using that definition, the
14 court found “that Power did not act ‘without permission’ within the meaning of Section 502 when
15 Facebook account holders utilized the Power website to access and manipulate their user content on
16 the Facebook website, even if such action violated Facebook’s Terms of Use.” *Id.* at *12. However,
17 the *Power Ventures* court did not base its construction of § 502 on any California state court
18 authority or on the statutory language. Rather, it concluded that Judge Seeborg’s interpretation of §
19 502 in *ConnectU* would give private entities too much “unbridled discretion to determine the scope
20 of criminal liability recognized under the statute” and would therefore raise constitutional concerns.
21 *Id.* at *8. While the Ninth Circuit decision in *Nosal* raised similar concerns, this Court fails to see
22 such a clear distinction between technical and non-technical restrictions on access; in either case, the
23 private entity arguably determines the scope of liability based on the level of restrictions it places on
24 a user’s access. Moreover, violations of access rules tend to be more discrete and delineated (as they
25 occur at the point of entry) than violation of use restrictions (which may occur after the fact over a
26 longer period of time). In any event, *Power Ventures*’s analysis does not consider circumstances
27 such as the Ninth Circuit described in *Brekka* and that in the instant case, in which a former
28

1 employee who has been terminated accesses the former employer's data without permission even
2 though his old log-in information might still be operable. *Brekka*, 581 F.3d at 1136.

3 Accordingly, at this early stage of the proceedings, the Court cannot conclude as a matter of
4 law based on the current limited briefing in the context of a Rule 15 the motion to amend that
5 Plaintiff's alleged conduct beyond his conditional access to Defendant's computer for the purpose of
6 obtaining files he did not have authority to access is outside the scope of § 502. This ruling,
7 however, is without prejudice to a Rule 56 motion for summary judgment with more complete
8 briefing and factual development regarding, *e.g.*, the level of access Plaintiff actually obtained,
9 whether Defendant actually placed any restrictions on said access, and whether the established
10 conduct in fact violated § 502.²

11 3. Conversion

12 Plaintiff next argues that Defendant's conversion claim fails to state a claim because it fails
13 to allege that he has "actually exercised dominion over any [Harland license] codes, nor that he ever
14 had possession of them nor that he ever disposed of Harland's property rights." *Opp.* at 6.
15 However, Defendant specifically alleges that Plaintiff accessed and copied and/or retained
16 Defendant's NPI and proprietary information, including the OnBase Software, for "use of such
17 information as the owner of Weingand CU Consulting or otherwise." *Am. Ans.* ¶¶ 38, 42. Thus,
18 while the pleading could likely contain more or better detail, it appears that it at least contains the
19 information Plaintiff argues is required. *See Han*, 2011 WL 5118748 at *4 (finding counterclaim
20 stated a claim for conversion where "Huawei has alleged that the company owned information
21 contained on the computer, that Han copied and erased some or all of that information, and that her
22 action caused damages").

23 4. Breach of Contract

24 Plaintiff next contends that Defendant's breach of contract claim fails because it does not
25 allege sufficient facts such as "when any contract was entered into, what the terms of the contract
26

27 ² Indeed, Plaintiff's counsel admitted at oral argument that the question of whether Plaintiff
28 exceeded his authorized access, as opposed to merely (allegedly) misused information to which he
had proper access, was a factual inquiry.

were, nor how they were breached.” Opp. at 7. However, the counterclaim states that Plaintiff was employed at Harland; that part of his “employment was governed in part by express and implied agreements,” including, *inter alia*, “the M&F Worldwide Corp. Code of Business Conduct”; that he agreed to be bound by said code of conduct in 2008, which included a duty to “maintain the secrecy of the Company’s confidential and proprietary information”; and that Plaintiff violated said code of conduct by accessing, copying, and failing to return said information after his employment was terminated. Am. Ans. ¶¶ 8-10, 14-22. Thus, Defendant has alleged a plausible claim for breach of contract.

5. Unjust Enrichment

Plaintiff argues that Defendant’s unjust enrichment claim is preempted by the Copyright Act because it concerns copyrightable material. *See* Opp. at 7 (citing *Seng-Tiong Ho v. Taflove*, 648 F.3d 489, 504 (7th Cir. 2011) (finding state law claims preempted because the “claims of conversion and fraud assert the same interests as those under the Copyright Act: to control the publication of the copyrighted work”). However, Defendant points out that some of the material involved is neither copyrightable nor related to publication of works in a way that might be construed as relating to the interests of the Copyright Act. This material includes confidential data such as social security numbers, addresses, and bank account information. *See* Reply at 5; *see also* *ConnectU LLC*, 489 F. Supp. 2d at 1092-93 (allegation that competitor gained unauthorized access to Facebook and misappropriated email addresses was not preempted by the Copyright Act).

In addition, to the extent Defendant’s claims are based on Plaintiff’s unauthorized copyrighted material, such as use of Defendant’s license and OnBase software, it is still not clear at this point whether such claims would be preempted. For example, “[m]ost courts have held that the Copyright Act does not preempt the enforcement of contractual rights.” *Altera Corp. v. Clear Logic, Inc.*, 424 F.3d 1079, 1089-90 (9th Cir. 2005) (“A state law tort claim concerning the unauthorized use of the software’s end-product is not within the rights protected by the federal Copyright Act.”). For purposes of a futility analysis, the Court need only determine that *some* “set of facts can be proved under the amendment that would constitute a valid claim or defense.” *Echostar*, 2009 WL

8398696 at *1 (quoting *Miller v. Rykoff-Sexton, Inc.*, 845 F.2d 209, 214 (9th Cir.1988)). Thus, on the current record, the claim is not futile.

6. Negligent Interferences with Prospective Economic Advantage

Plaintiff next claims that the negligent interference with prospective economic advantage claim is futile because it does not comply with the particularity requirements of Rule 9(b). Opp. at 8. However, Rule 9(b) does not apply to a claim of a *negligent* interference – Defendant’s claim focuses on Plaintiff’s alleged “accessing [of] NPI belonging to the clients of Harland’s customers, which he knew or should have known would disrupt and harm Harland’s relationships with its customers.” Am. Ans. ¶ 59. Defendant further alleges that “[a]s a result of Weingand’s conduct, these relationships were actually disrupted such that Harland was required to provide notice to its customers regarding Weingand’s access of their NPI.” *Id.* Defendant does not appear to allege any *fraudulent* interference or misrepresentations with respect to this claim. *Cf. Meridian Project Sys., Inc. v. Hardin Const. Co., LLC*, 404 F. Supp. 2d 1214, 1219 (E.D. Cal. 2005) (finding Rule 9(b) applied because intentional interference and other claims were “based on the common allegations that counterdefendants *intentionally* misrepresented to CMIC’s prospective customers that CMIC had infringed Meridian’s copyright, in order to dissuade the customers from purchasing CMIC’s software products”) (emphasis added). In addition, to the extent that particularity is required, Defendant has arguably complied with that requirement by detailing exactly when Plaintiff accessed and copied the relevant software and files and what those files are.

7. UCL

Finally, Plaintiff argues that Defendant’s UCL claim similarly fails because it falls short of the Rule 9(b) particularity requirement. To the extent that Defendant states claims for statutory violations described above, those would also constitute unlawful business practices under the UCL not subject to Rule 9(b). To the extent that particularity is required for any unfair or fraudulent claims, as noted above, Defendant has provided significant detail as to when, where, and what Plaintiff accessed and copied.

Accordingly, at this point, the Court cannot conclude that Defendant’s proposed amendments are futile.

1 C. Undue Delay

2 Plaintiff next argues that Defendant should not be permitted to amend its answer due to
3 undue delay, as Defendant's initial answer was filed on June 23, 2011. "Relevant to evaluating the
4 delay issue is whether the moving party knew or should have known the facts and theories raised by
5 the amendment in the original pleading." *Jackson v. Bank of Hawaii*, 902 F.2d 1385, 1388 (9th Cir.
6 1990) (citations omitted).

7 In the instant case, Defendant provides sufficient information to justify its delay in seeking to
8 amend. Specifically, Defendant states that it began investigating Plaintiff's potential unauthorized
9 access after receiving his first production of documents in October of 2011. At that time, Defendant
10 noticed a discrepancy between the Performance Improvement Plan ("PIP") Plaintiff produced in
11 discovery and the version Human Resources had on file that Plaintiff had submitted in October of
12 2010 (while he was still employed at Harland). Svanfeldt Decl. ¶ 4. Defendant also discovered
13 information that Plaintiff had failed to produce in discovery, including a LinkedIn resume indicating
14 that he had been an owner/consultant for Weingand CU Consulting since his Harland employment
15 ended, and that his resume advertised his use of OnBase and other software. *Id.* ¶ 5.

16 After receiving these discovery responses, Defense counsel continued to meet and confer
17 with Plaintiff's counsel regarding further discovery, and served a second set of requests for
18 production in December 2011. *Id.* ¶ 15. Defendant also engaged a forensic analyst (Lynell Phillips)
19 to "determine what activity took place on the Company computer Mr. Weingand accessed on
20 November 6, 2010 and to locate any and all versions [of] his PIP." *Id.* ¶¶ 9-12. Ms. Phillips found
21 that Mr. Weingand had accessed 2,755 files from 1:11 p.m. to 1:41 p.m. on November 6, 2010, after
22 his termination. *Id.* ¶ 16. Defendant informed Plaintiff of these findings on January 3, 2012, and
23 stated that said files included confidential and proprietary information. *Id.* ¶ 17. The parties
24 subsequently exchanged numerous meet and confer letters regarding disputes over Plaintiff's
25 compliance with Defendant's discovery requests and whether Plaintiff was obligated to produce the
26 storage device he used on the company computer in November 2010. *Id.* ¶¶ 17-23. Plaintiff
27 produced supplemental discovery responses, including a version of his PIP, on January 27, 2012.
28

1 Defendant informed the Court of its forensic analyst's findings on March 16, 2012, and the
2 Court gave Defendant until April 17 to file its stipulated amended answer or a motion for leave to
3 amend. Defendant requested that the analyst prepare a formal report based on her findings, which
4 Defendant received on April 13, 2012. Defendant shared its proposed amended answer and
5 counterclaims with Plaintiff and April 16, and when Plaintiff refused to stipulate to its filing, filed
6 this motion for leave on April 17.

7 Plaintiff asserts that Defendant has unreasonably delayed filing the instant motion because it
8 should have known the basis for its claims when Plaintiff actually visited the office on November 6,
9 2010. Opp. at 10-11. However, that Defendant knew (or should have known) Plaintiff obtained
10 access to Harland computers to download "personal files," Svanfeldt Decl. ¶ 11, would not
11 necessarily have triggered an investigation into what files Plaintiff accessed. Rather, Defendant
12 began such an investigation when it first had a reason to suspect Plaintiff may have accessed files in
13 excess of his authorization – when it received conflicting versions of documents in discovery. Once
14 the investigation began, Defendant provides sufficient detail as to each step of its investigation and
15 meet and confer attempts to demonstrate that it acted with reasonable diligence.

16 In *Han*, the court credited the defendant employer's statement that it had discovered the
17 claim "when it hired a computer forensic firm in connection with disclosures required by the
18 already-existing litigation." *Han*, 2011 WL 5118748 at *3. The court found that this explanation
19 was reasonable and did not indicate an undue delay. *See also Trimble Navigation Ltd. v. RHS, Inc.*,
20 C 03-1604 PJH, 2007 WL 2727164 (N.D. Cal. Sept. 17, 2007) (five months between discovery of
21 potential basis for counterclaim and filing of motion was justified because defendants were engaging
22 in investigation "to be sure of all necessary facts in as reasonable a time as possible, before seeking
23 leave to amend"). *Cf. AmerisourceBergen Corp. v. Dialysist West, Inc.*, 465 F.3d 946, 953 (9th
24 Cir.2006) (eight-month delay between discovery of claim and filing of motion for leave to amend
25 was unreasonable). Here, Defendant has pursued multiple avenues to obtain information as to
26 Plaintiff's conduct before attempting to amend its pleadings, and has complied with the Court's
27 order as to when it must seek leave to amend. On this record, there is no showing of undue delay.
28

1 D. Prejudice

2 Finally, Plaintiff argues that amendment would prejudice him because it would change the
3 nature and scope of the action from an employment-based suit to a computer fraud suit. “[I]t is the
4 consideration of prejudice to the opposing party that carries the greatest weight” in considering a
5 motion for leave to amend. *Eminence Capital, LLC v. Aspeon, Inc.*, 316 F.3d 1048, 1052 (9th Cir.
6 2003). However, Plaintiff bears the burden of showing prejudice. *Id.* (citations omitted).


7 In this case, the fact that Defendant seeks to assert counterclaims that differ in scope from
8 Plaintiff’s initial pleadings does not demonstrate prejudice. In fact, the court in *Han* rejected just
9 such an argument under similar facts, finding that “[a]lthough the counterclaims will introduce new
10 issues, a plaintiff has no right to pre-emptive protection from counterclaims merely because she
11 wishes the litigation to focus on her own claims.” *Jun Han v. Futurewei Technologies, Inc.*,
12 11-CV-831-JM JMA, 2011 WL 5118748, at *3 (S.D. Cal. Oct. 28, 2011). Nor has Plaintiff made
13 any showing of prejudice based on the timing of the proposed amendments, as discovery is still open
14 and no dispositive motions are pending. *Cf. M/V Am. Queen v. San Diego Marine Const. Corp.*, 708
15 F.2d 1483, 1492 (9th Cir. 1983) (finding undue delay and prejudice in part because “a motion for
16 summary judgment was pending and possible disposition of the case would be unduly delayed by
17 granting the motion for leave to amend”).

18 Accordingly, the Court **GRANTS** Defendant’s motion for leave to file an amended answer
19 and counterclaims.

20 This order disposes of Docket No. 29.

21
22 IT IS SO ORDERED.

23
24 Dated: June 19, 2012

25 
EDWARD M. CHEN
United States District Judge